IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Russell D. Housley et al.

Assignee: Spyrus, Inc.

Title: Customizable Cryptographic Device

Serial No.: Unknown Filed: Herewith

Examiner: M. Smithers Group Art Unit: 2132

Attorney Docket No.: SPY-007-C1

Milpitas, California
February 15, 2002

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Please enter the following preliminary amendment in the above-identified application. Appended to this Amendment is a document entitled Version with Markings to Show Changes Made, showing the changes made to the specification, claims and abstract of this application in this Amendment.

IN THE SPECIFICATION

The title has been amended as follows: SECURE, EASY AND/OR IRREVERSIBLE CUSTOMIZATION OF CRYPTOGRAPHIC DEVICE

Please replace the paragraph beginning at page 4, line 29, with the following rewritten paragraph:

For example, in one embodiment of the invention, a computer readable storage medium includes stored thereon: i) a first set of code (i.e., instructions and/or

data) used to perform one or more sub-operations (which can be, for example, one or more mathematical primitive operations); ii) a second set of code, distinct from the first set of code, used to perform one or more cryptographic operations, the second set of code including one or more instructions that cause performance of instructions and/or use of data from the first set of code so that the one or more sub-operations are performed; and iii) a third set of code for allowing and mediating access to the first set of code from a device external to a device of which the computer readable storage medium is part. The computer readable storage medium can be a data storage device or devices that, together with a processor, can be embodied in a cryptographic device to flexibly provide cryptographic operations in the cryptographic device.

Please replace the paragraph beginning at page 5, line 13, with the following rewritten paragraph:

This embodiment of the invention enables easy and secure modification (expansion, reduction or changing) of application code via the exposure of, for example, the mathematical primitive operations available on a particular cryptographic device. In particular, this embodiment of the invention enables modification of available cryptographic operations at a relatively high level of programming abstraction, thus enabling such modification to be accomplished relatively easily. Further, this embodiment of the invention enables the modification to be accomplished in

a manner that does not necessitate or allow access by the application developer to other operations of the cryptographic device, thus providing security for the proprietary code and/or cryptographic keys of other persons or entities that may be present on the cryptographic device. Additionally, this embodiment of the invention can allow storage of a part of the code for the cryptographic operations that need never change in a small and unmodifiable storage device (ROM), while a part of the code of the cryptographic operations that it may desired to change is stored in a larger and modifiable storage device (EEPROM), thus retaining the capability of modifying the cryptographic operations present on a cryptographic device, while minimizing or eliminating any limitation on the number and/or complexity of the cryptographic operations that can be provided in the cryptographic device.

Please replace the paragraph beginning at page 8, line 2, with the following rewritten paragraph:

FIG. 4 is a block diagram of the functional components of a cryptographic device 400 according to an embodiment of the invention. The block 401 (hereinafter sometimes referred to as "the mathematical primitives storage area") represents instructions and/or data ("code") that enables the performance of one or more mathematical primitive operations. The block 402 (hereinafter sometimes referred to as "the cryptographic operations storage area") represents code that enables the performance of one or more

cryptographic operations. In general, the block 402 does not include code that enables the performance of mathematical primitive operations. The block 403 (hereinafter sometimes referred to as "the cryptographic characteristic table") represents data ("access permission data") that specifies cryptographic characteristics in accordance with which one or more of the mathematical primitive operations or cryptographic operations are performed. The block 404 represents code (hereinafter sometimes referred to as "the access allowance verifier") that, using the access permission data, controls access by a user to the mathematical primitive operations and cryptographic operations. Finally, the block 405 represents code (hereinafter sometimes referred to as "the key manager") for storing and accessing cryptographic keys and certificates.

Please replace the paragraph beginning at page 8, line 26, with the following rewritten paragraph:

In general, requests by application code 406 for performance of cryptographic operations are received by the access allowance verifier 404 from the application code interface 407. Each request is evaluated by the access allowance verifier 404 to ensure that the request is allowable. Whether a request is allowable is evaluated by comparing the cryptographic characteristics associated with the request to the availability of such cryptographic characteristics, as indicated by the access permission data

stored in the cryptographic characteristic table 403. If the request is allowable, then cryptographic operations are performed in accordance with the request, as described further below.

Please replace the paragraph beginning at page 10, line 10, with the following rewritten paragraph:

Preferably, the access permission data of the cryptographic characteristic table 403 are stored in a programmable read-only memory (PROM). The use of such a data storage device enables flexibility in establishing the access permission data (i.e., the availability of cryptographic characteristics) of a cryptographic device, since the access permission data can be established at device fulfillment (see FIG. 1). Thus, a single mass-produced type of cryptographic device can be tailored to meet cryptographic needs for many different applications. Further, the use of such a data storage device enables permanency - and, therefore, security - in establishing the access permission data of a cryptographic device, since once the access permission data are established, the access permission data cannot be changed. Thus, a single mass-produced type of cryptographic device can be tailored to satisfy domestic demand for robust cryptographic capabilities or to conform to export regulations dictating somewhat less robust cryptographic capabilities, while, in the latter case, providing confidence that the limitations

on the cryptographic capabilities cannot be circumvented once the cryptographic device has been exported to a user.

Please replace the paragraph beginning at page 16, line 13, with the following rewritten paragraph:

The cryptographic operations storage area 402 can include any desired cryptographic operations. For example, the cryptographic operations included in the cryptographic operations storage area 402 can include, but are not limited to, the following operations: RSA encrypt, RSA decrypt, DSA sign, DSA verify, 3-key triple DES, Diffie-Hellman and elliptic curve. However, it is emphasized that any other cryptographic operations, including, in particular, cryptographic operations that are developed in the future, can be included in the cryptographic operations storage area 402. It is an important aspect of the invention that any cryptographic operation can be easily implemented in a cryptographic device according to the invention.

IN THE DRAWINGS

Applicants request permission to amend FIG. 4 as indicated in red on a copy of FIG. 4 as originally filed that is enclosed with this Response.

IN THE CLAIMS

Please amend the claims as follows:

1. (Amended) A cryptographic device, comprising:

means for performing one or more cryptographic operations; and

a data storage device or devices for storing access permission data representing the availability of one or more cryptographic characteristics in accordance with which one or more of the cryptographic operations are performed, wherein all of the access permission data of the cryptographic device is stored in the data storage device or devices such that once a value or values of the access permission data are stored in the data storage device or devices, the value or values of the access permission data cannot be changed.

4. (Amended) A computer readable storage medium encoded with instructions and/or data, comprising:

instructions and/or data for performing one or more cryptographic operations; and

access permission data stored in accordance with a predefined data structure, the access permission data representing an availability of one or more cryptographic characteristics in accordance with which one or more cryptographic operations are performed by a cryptographic device, wherein all of the access permission data is stored in the storage medium such that once a value or values of

the access permission data are stored in the storage medium, the value or values of the access permission data cannot be changed.

6. (Amended) A cryptographic device, comprising:

a processor for executing instructions and/or accessing data to perform one or more cryptographic operations that each necessitate the performance of one or more sub-operations;

one or more data storage devices for storing a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation, and a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and

means for allowing access to the first set of instructions and/or data from a device external to the cryptographic device.

14. (Amended) A computer readable storage medium encoded with one or more computer programs for enabling performance of cryptographic operations, comprising:

a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation;

a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and

a third set of instructions and/or data for allowing access to the first set of instructions and/or data from a device external to a cryptographic device of which the computer readable storage medium is part.

15. (Amended) A computer readable storage medium as in Claim 14, wherein the one or more sub-operations comprise one or more mathematical primitive operations.

17. (Amended) A computer readable storage medium as in Claim 14, wherein the cryptographic operations include one or more of the following: RSA encrypt, RSA decrypt, DSA sign, DSA verify, Diffie-Hellman and elliptic curve.

Please enter the following new claims:

18. (New) A computer readable storage medium as in Claim 4, further comprising a programmable read-only memory for storing the access permission data.

19. (New) A cryptographic device as in Claim 6, further comprising means for controlling access to the first and second sets of instructions and/or data, wherein:

the means for controlling access to the first and second set of instructions and/or data comprises the means for allowing access to the first set of instructions and/or data; and

the means for allowing access to the first set of instructions and/or data does not enable access to the second set of instructions and/or data.

20. (New) A computer readable storage medium as in Claim 14, further comprising a fourth set of instructions and/or data for controlling access to the first and second sets of instructions and/or data, wherein:

the fourth set of instructions and/or data comprises the third set of instructions and/or data; and

the third set of instructions and/or data does not enable access to the second set of instructions and/or data.

IN THE ABSTRACT

The title on the abstract page has been amended as follows: SECURE, EASY AND/OR IRREVERSIBLE CUSTOMIZATION OF CRYPTOGRAPHIC DEVICE

REMARKS

Claims 1-17 were pending. Claims 1, 4, 6, 14, 15 and 17 have been amended. Claims 18-20 have been added. Allowance of Claims 1-20 is requested. If the Examiner wishes to discuss any aspect of this application, the Examiner is invited to telephone Applicants' undersigned attorney at (408) 945-9912.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on February 15, 2002.

2-15-02 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham
David R. Graham
Reg. No. 36,150
Attorney for Applicants

Version with Markings to Show Changes Made

(Additions are underlined, deletions are enclosed in brackets)

In the specification:

The title has been amended as follows: [CUSTOMIZABLE CRYPTOGRAPHIC DEVICE] SECURE, EASY AND/OR IRREVERSIBLE CUSTOMIZATION OF CRYPTOGRAPHIC DEVICE

The paragraph beginning at page 4, line 29 has been amended as follows:

For example, in one embodiment of the invention, a computer readable storage medium includes stored thereon: i) a first set of code (i.e., instructions and/or data) used to perform one or more [sub operations] sub-operations (which can be, for example, one or more mathematical primitive operations); ii) a second set of code, distinct from the first set of code, used to perform one or more cryptographic operations, the second set of code including one or more instructions that cause performance of instructions and/or use of data from the first set of code so that the one or more sub-operations are performed; and iii) a third set of code for allowing and mediating access to the first set of code from a device external to a device of which the computer readable storage medium is part. The computer readable storage medium can be a data storage device or devices that, together with a processor, can be embodied in a cryptographic device to flexibly provide cryptographic operations in the cryptographic device.

The paragraph beginning at page 5, line 13 has been amended as follows:

This embodiment of the invention enables easy and secure modification (expansion, reduction or changing) of [the] application code via the exposure of, for example, the mathematical primitive operations available on a particular cryptographic device. In particular, this embodiment of the invention enables modification of available cryptographic operations at a relatively high level of programming abstraction, thus enabling such modification to be accomplished relatively easily. Further, this embodiment of the invention enables the modification to be accomplished in a manner that does not necessitate or allow access by the application developer to other operations of the cryptographic device, thus providing security for the proprietary code and/or cryptographic keys of other persons or entities that may be present on the cryptographic device. Additionally, this embodiment of the invention can allow storage of a part of the code for the cryptographic operations that need never change in a small and unmodifiable storage device (ROM), while a part of the code of the cryptographic operations that it may desired to change is stored in a larger and modifiable storage device (EEPROM), thus retaining the capability of modifying the cryptographic operations present on a cryptographic device, while minimizing or eliminating any limitation on the number and/or complexity of the cryptographic operations that can be provided in the cryptographic device.

The paragraph beginning at page 8, line 2 has been amended as follows:

FIG. 4 is a block diagram of the functional components of a cryptographic device 400 according to an embodiment of the invention. The block 401 (hereinafter sometimes referred to as "the mathematical primitives storage area") represents instructions and/or data ("code") that enables the performance of one or more mathematical primitive operations. The block 402 (hereinafter sometimes referred to as "the cryptographic operations storage area") represents code that [enable] <u>enables</u> the performance of one or more cryptographic operations. In general, the block 402 does not include code that enables the performance of mathematical primitive operations. The block 403 (hereinafter sometimes referred to as "the cryptographic characteristic table") represents data ("access permission data") that specifies cryptographic characteristics in accordance with which one or more of the mathematical primitive operations or cryptographic operations are performed. The block 404 represents code (hereinafter sometimes referred to as "the access allowance verifier") that, using the access permission data, controls access by a user to the mathematical primitive operations and cryptographic operations. Finally, the block 405 represents code (hereinafter sometimes referred to as "the key manager") for storing and accessing cryptographic keys and certificates.

The paragraph beginning at page 8, line 26 has been amended as follows:

In general, requests by application code 406 for performance of cryptographic operations are received by the access allowance verifier 404 from the application code interface 407. Each request is evaluated by the access allowance verifier 404 to ensure that the request is allowable. Whether a request is allowable is evaluated by comparing the cryptographic characteristics associated with the request to the availability of such cryptographic characteristics, as indicated by the access permission data stored in the cryptographic characteristic table 403. If the request is allowable, then cryptographic operations are performed in accordance with the request, as described further below.

The paragraph beginning at page 10, line 10 has been amended as follows:

Preferably, the access permission data of the cryptographic characteristic table 403 are stored in a programmable read-only memory (PROM)[, e.g., the PROM 404 of the computational device 400 (FIG. 4)]. The use of such a data storage device enables flexibility in establishing the access permission data (i.e., the availability of cryptographic characteristics) of a cryptographic device, since the access permission data can be established at device fulfillment (see FIG. 1). Thus, a single mass-produced type of cryptographic device can be tailored to meet cryptographic needs for many different applications.

Further, the use of such a data storage device enables permanency - and, therefore, security - in establishing the access permission data of a cryptographic device, since once the access permission data are established, the access permission data cannot be changed. Thus, a single mass-produced type of cryptographic device can be tailored to satisfy domestic demand for robust cryptographic capabilities or to conform to export regulations dictating somewhat less robust cryptographic capabilities, while, in the latter case, providing confidence that the limitations on the cryptographic capabilities cannot be circumvented once the cryptographic device has been exported to a user.

The paragraph beginning at page 16, line 13 has been amended as follows:

The cryptographic operations storage area 402 can include any desired cryptographic operations. For example, <u>the cryptographic operations included in</u> the cryptographic operations storage area 402 can include, but are not limited to, the following operations: RSA encrypt, RSA decrypt, DSA sign, DSA verify, 3-key triple DES, Diffie-Hellman and elliptic curve. However, it is emphasized that any other cryptographic operations, including, in particular, cryptographic operations that are developed in the future, can be included in the cryptographic operations storage area 402. It is an important aspect of the invention that any cryptographic operation can be

easily implemented in a cryptographic device according to the invention.

In the claims:

Claims 1, 4, 6, 14, 15 and 17 have been amended as follows:

1. (Amended) A cryptographic device, comprising:

means for performing one or more cryptographic operations; and

a data storage device or devices for storing access permission data representing [an] the availability of one or more cryptographic characteristics in accordance with which one or more of the cryptographic operations are performed, wherein all of the access permission data of the cryptographic device is stored in the data storage device or devices such that once a value or values of the access permission data are stored in the data storage device or devices, the value or values of the access permission data cannot be changed.

4. (Amended) A computer readable storage medium encoded with instructions and/or data, comprising:

instructions and/or data for performing one or more cryptographic operations; and

[on which] access permission data [is] stored in accordance with a predefined data structure, the access permission data representing an availability of one or more cryptographic characteristics in accordance with which one

or more [of] cryptographic operations are performed by a cryptographic device, wherein all of the access permission data is stored in the storage medium such that once a value or values of the access permission data are stored [on] in the storage medium, the value or values of the access permission data cannot be changed.

6. (Amended) A cryptographic device, comprising:

a processor for executing instructions and/or accessing data to perform one or more cryptographic operations that each necessitate the performance of one or more sub-operations; [and]

one or more data storage devices for storing a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation, and a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and

means for allowing access to the first set of instructions and/or data from a device external to the cryptographic device.

14. (Amended) A computer readable storage medium encoded with one or more computer programs for enabling performance of cryptographic operations, comprising:

a first set of instructions and/or data used to perform one or more [sub-primitive operations] sub-operations of a cryptographic operation; [and]

a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the [sub-sub-operations] sub-operations are performed; and

a third set of instructions and/or data for allowing [and mediating] access to the first set of instructions and/or data from a device external to a cryptographic device of which the computer readable storage medium is part.

15. (Amended) A [cryptographic device] computer readable storage medium as in Claim 14, wherein the one or more sub-operations comprise one or more mathematical primitive operations.

17. (Amended) A computer readable storage medium as in Claim [13] 14, wherein the cryptographic operations include one or more of the following: RSA encrypt, RSA decrypt, DSA sign, DSA verify, Diffie-Hellman and elliptic curve.

Claims 18-20 have been added as follows:

18. (New) A computer readable storage medium as in Claim 4, further comprising a programmable read-only memory for storing the access permission data.

19. (New) A cryptographic device as in Claim 6, further comprising means for controlling access to the first and second sets of instructions and/or data, wherein:

the means for controlling access to the first and second set of instructions and/or data comprises the means for allowing access to the first set of instructions and/or data; and

the means for allowing access to the first set of instructions and/or data does not enable access to the second set of instructions and/or data.

20. (New) A computer readable storage medium as in Claim 14, further comprising a fourth set of instructions and/or data for controlling access to the first and second sets of instructions and/or data, wherein:

the fourth set of instructions and/or data comprises the third set of instructions and/or data; and

the third set of instructions and/or data does not enable access to the second set of instructions and/or data.

In the abstract:

The abstract has been amended as follows:

[CUSTOMIZABLE CRYPTOGRAPHIC DEVICE] SECURE, EASY AND/OR IRREVERSIBLE CUSTOMIZATION OF CRYPTOGRAPHIC DEVICE

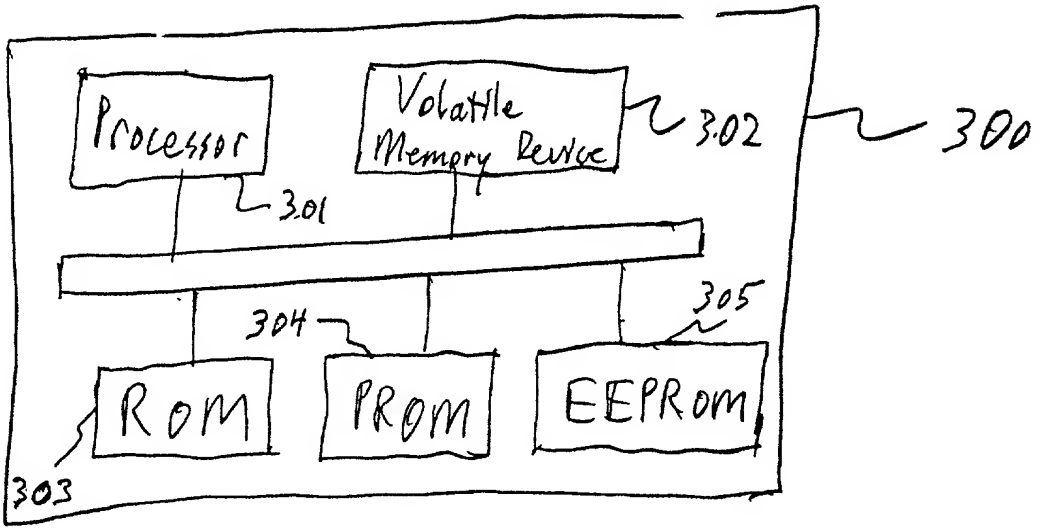
Processor
Volatile Memory Device
302
300
301
304
305
ROM
PROM
EEPROM
303

FIG. 3.

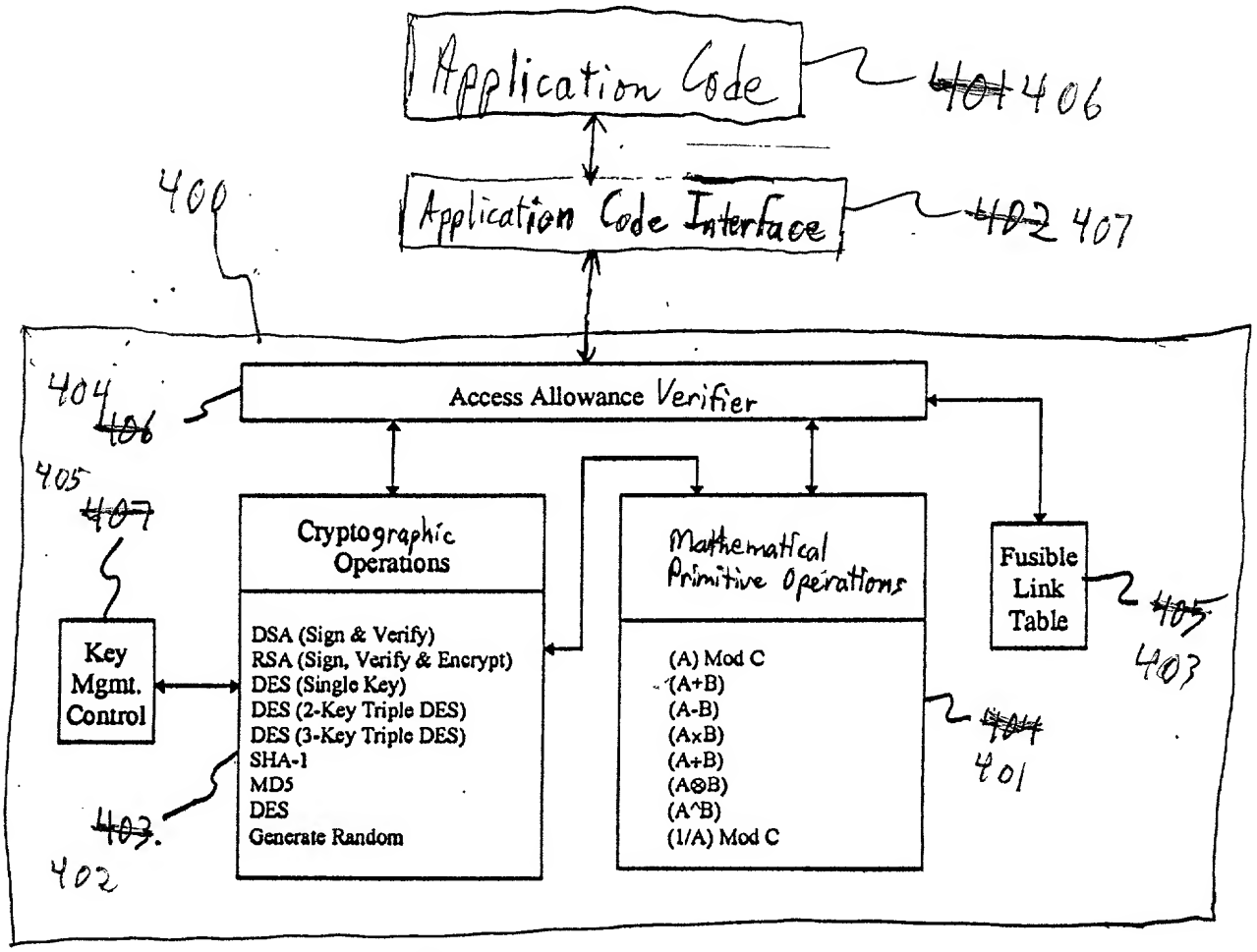
Application Code
406
Application Code Interface
407
400
Access Allowance Verifier
404
405
Key Mgmt. Control
Cryptographic Operations
DSA (Sign & Verify)
RSA (Sign, Verify & Encrypt)
DES (Single Key)
DES (2-Key Triple DES)
DES (3-Key Triple DES)
SHA-1
MD5
DES
Generate Random
403
402
Mathematical Primitive Operations
(A) Mod C
(A+B)
(A-B)
(AxB)
(A+B)
(A⊗B)
(A^B)
(1/A) Mod C
401
Fusible Link Table
405
403

FIG. 4